

Appl. No. 09/720,353
Amendment dated April 8, 2005
Reply to Office Action of January 13, 2005

REMARKS

Claims 2 - 11 are pending in the instant application. In the first Office Action, Claims 1 - 7 had been rejected under 35 U.S.C. § 102(a) as being anticipated by U.S. Patent No. 6,496,928 to Deo et al. (hereinafter "Deo") and Claim 8 had been rejected under 35 U.S.C. § 103(a) as being unpatentable over Deo in view of U. S. Patent No. 6,009,410 to Horstmann (hereinafter "Horstmann"). Claims 2 - 4 and 9 have been previously amended by an amendment on June 30, 2004, and Claims 5 - 8 and 10 were previously amended by a Preliminary Amendment on December 21, 2000. Claim 1 has been cancelled and replaced with amended Claim 11, in an amendment on June 30, 2004.

In the Second Office Action, Claims 2 - 7, 9 and 11 have been rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by U.S. Patent No. 5,608,800 to Hoffmann et al. (hereinafter "Hoffmann"). Claim 8 has been rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Hoffmann in view of the Horstmann reference. Claim 10 has been rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Hoffmann in view of Official Notice. The rejections are traversed and reconsideration is respectfully requested.

Claims 2 - 8 and 11 have been rejected under 35 U.S.C. § 112 second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter claimed. The Examiner rejected Claim 7 asserting that the term "in advance" is not understood. Claim 7 has been amended to address the Examiner's rejection. Claim 11 also has been amended to address the issues raised by the Examiner, with the exception of adding the step of signing a message which the applicant contends is not required. A specific step of signing the message is not required because the Specification discloses that the sender forms a data set which contains the sequence number, the message and the signature, rather than literally signing the message. The message is, in effect, "signed" when the signature and the message are formed into a data set. Claim 11 has been amended to clarify this by

Appl No. 09/720,353
Amendment dated April 8, 2005
Reply to Office Action of January 13, 2005

adding the step of creating the data set. This is supported in the Specification at page 6 lines 7 – 8.

The Examiner rejected Claims 2 through 8 asserting that they depend upon canceled Claim 1. Claims 2 - 8 have been amended to delete the dependency on cancelled Claim 1 and make these claims dependant on Claim 11. The Abstract has been amended. No new matter has been added.

Claims 11, 9 and 2 – 7 have been rejected under 35 U.S.C. § 102(b) as being anticipated by the Deo reference. The rejections are traversed and reconsideration is respectfully requested.

The Deo reference discloses a system including a content provider 12, a wireless carrier 14, a computer 16 and a mobile device 18 (Fig. 1). The content provider 12 provides any suitable data from a database. Examples of such data include news, stock quotes, traffic reports, weather information and sports data. The wireless carrier 14 is configured to receive data from the content provider via dial-up or direct internet connection. The mobile device 18 includes a receiver 22, a modem 24, a synchronization component 28, a keyboard and a display. The data can be transmitted from the content provider 12 to the wireless carrier 14 to the mobile device 18. The data can also be transmitted from the content provider 12 to a computer 16 to the mobile device 18. The data can also be transmitted directly from the content provider 12 to the mobile device 18 (Deo reference column 1 lines 66 and 67, column 2 lines 1 – 67, column 6 lines 18 – 26). The content provider 12 and the wireless carrier are configured to program the mobile device 18 with an encryption key for decrypting a content message (Deo reference column 22 lines 57 – 60). Programming of the mobile device 18 includes a user of the mobile device 18 requesting a subscription to receive data; the content provider 12 requesting the wireless carrier 14 to program a code into the mobile device; content provider 12 passing the identity of the user's mobile device 18; the wireless carrier 14 generates a temporary key; the wireless carrier 14 transmits the temporary key to the content

Appl. No. 09/720,353
 Amendment dated April 8, 2005
 Reply to Office Action of January 13, 2005

provider 12; wireless carrier 14 prepares an encrypted program message using a secret key known only to the wireless carrier 14 and the mobile device 18; the wireless carrier 14 transmits the encrypted program message to the mobile device 18.

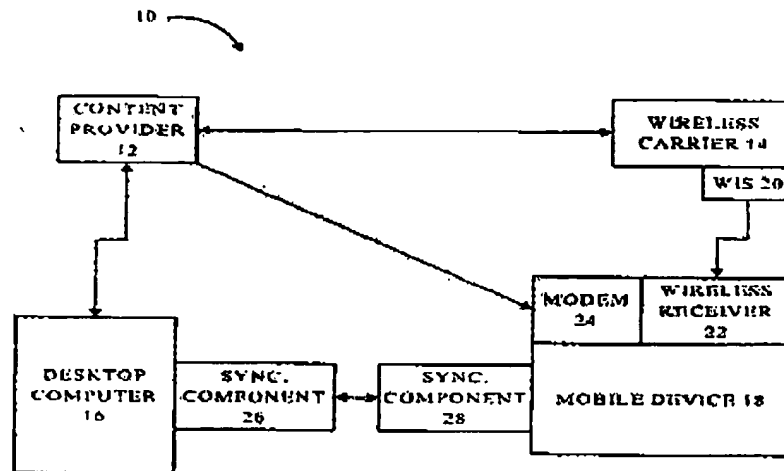


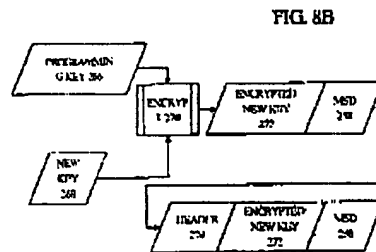
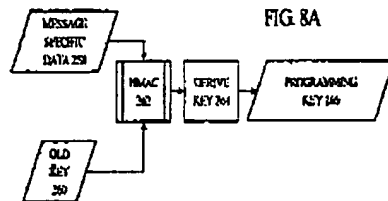
FIG. 1

The Deo reference also discloses a method of controlling access to a content message received by a plurality of mobile devices 18. The method disclosed in the Deo reference includes providing the mobile device 18 with a broadcast encryption key (new key 268). Prior to broadcasting, a message is encrypted using the new key resulting in an encrypted message. The encrypted message is modified resulting in a content message. The mobile device 18 having the new key is configured to decrypt the content message. The content message is then broadcast.

The Deo reference includes a hash message authentication code (HMAC) generator 262, wherein the HMAC generator derives a first hash value that is used for biasing a key derivation algorithm (Fig. 8A). The first hash value depends on a first set of Message Specific Data (MSD) 258 and an old key 260, wherein the first hash value and the first set of MSD are provided by a cryptography component to

Appl. No. 09/720,353
 Amendment dated April 8, 2005
 Reply to Office Action of January 13, 2005

the HMAC generator 262. The key derivation algorithm is then provided to a key derivation component 264, wherein the key derivation component acts upon the key derivation algorithm to derive a programming key 266. The programming key 266 is used to encrypt a new key 268 (Fig. 8B). A second set of MSD 294 and the new key 268 are transmitted to the HMAC generator 262, wherein the HMAC generator derives a second hash value. The second hash value is transmitted to the key derivation component 264 to create a message specific key 296. (Deo reference Fig. 9A and column 24 lines 32 – 58, column 26 lines 7 – 23). A message 298 is encrypted with the message specific key 296 in order to obtain an encrypted message 300. A third set of MSD 298 and a header 302 are added to the encrypted message 300 resulting in generation of a content message 304 (Fig. 9B). The content message 304 is broadcast to the mobile device 18. The mobile device is provided with the new key 268 and the content message 304. The content message 304 is decrypted on the mobile device 18 using the new key 268.



Appl. No. 09/720,353
 Amendment dated April 8, 2005
 Reply to Office Action of January 13, 2005

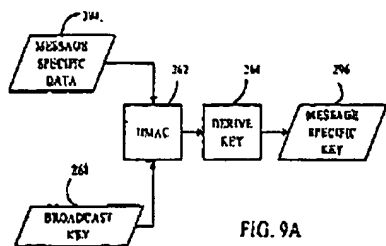


FIG. 9A

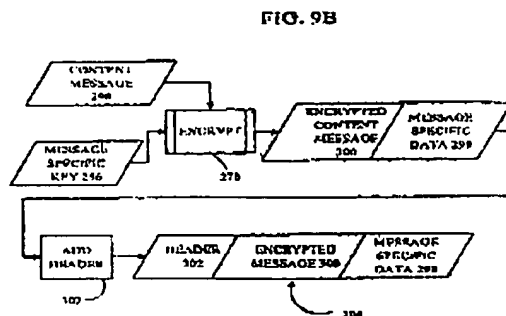


FIG. 9B

The Examiner asserts that the HMAC generator disclosed in the Deo reference reads on the one-time encrypter disclosed in Claim 11 of the current application (second Office Action sec. 5).

The Applicant disagrees with the Examiner's argument that Deo teaches a one-time encrypter. The pertinent clause from Claim 11 reads as follows: "using one of the sequence numbers and the main key to create a signing key by means of a one-time encryption." The one-time encryption disclosed in Claim 11 of the present application is distinct from the Deo disclosure of a hashed message authentication code (HMAC) generator. The Deo HMAC generator derives hash values and does not create a signing key by means of one-time encryption as disclosed in Claim 11 of the present application. Furthermore, the Deo invention discloses use of multiple keys (i.e., old key, new key, and programming key) to create a message specific key, rather than a shared main key utilizing one-time encryption as disclosed in Claim 11 of the current application. In addition, the Deo reference disclosure of an HMAC generator which derives hash values is distinguishable from using sequence numbers to create a signing key as recited in Claim 11 of the current application.

The Examiner asserts that the Applicant provides no specifics supporting the argument that "the elements of Claim 11 and the order in which they are presented are not present in the Deo reference" (second Office Action sec. 6). The order in which the method steps of Claim 11 are presented is distinct from the method

Appl No. 09/720,353
Amendment dated April 8, 2005
Reply to Office Action of January 13, 2005

disclosed in the Deo reference as evidenced from the description of the Deo process detailed above. In particular it is evident that the Deo reference discloses that a broadcast key is stored in a mobile device after it is generated in accordance with Deo, rather than disclosing a first step of "initializing a control center and a receiver with a shared main key," as set forth in Claim 11 as amended herein.

The Examiner rejects Applicant's argument that Deo does not disclose a control center having a first memory for a secret key, stating that memory is inherently used in the process as disclosed in Deo. The Examiner also asserts that the Deo reference teaches a control center (i.e., content provider) wherein the control center produces a signing key by means of one time encryption (second Office Action sec. 7). The inherency of memory is irrelevant. Instead, what distinguishes the Deo reference from the current application is that Claim 11 discloses a control center and a receiver which share the same key. The Deo reference discloses a secret key known only to the sender (wireless carrier 14) and the receiver (mobile device 18). This teaches away from the invention recited in Claim 11 as amended herein. The only manner by which the Examiner can make the mental leap from Deo to the invention recited in Claim 11 is via hindsight based upon the disclosure of the Applicant's patent application. This is impermissible. The Deo reference states that "only the authorized mobile devices have this key," which teaches directly away from sharing the same key as recited in the current application (Deo column 26 lines 10 and 11). Since the Deo reference indicates that the control center (content provider 12) first must obtain the key 268 which is stored on the mobile device 18 (receiver), it is further evident that Deo teaches away from a control center and a receiver which share the same key (Deo column 26 lines 7 and 8). Since the Deo control center must obtain the key, it could not possibly have had the key to share.

In addition, the content provider disclosed in Deo is distinct from the control center claimed in the current application in that the Deo content provider does not "produce one or more sequence numbers; using one of the sequence numbers and

Appl. No. 09/720,353
Amendment dated April 8, 2005
Reply to Office Action of January 13, 2005

the main key to create a signing key by means of a one-time encryption; providing the signing key and the sequence number to the sender via a secure transmission." Instead the Deo content provider 12 requests the wireless carrier 14 to program a code into the mobile device (Deo column 23 lines 33 – 36).

The Examiner rejects the Applicant's argument that Deo does not disclose a receiver containing a corresponding memory that contains a common key asserting that the Deo reference discloses a receiver using a one time encryption and a main key to decrypt messages (second Office Action sec. 8). The Examiner also asserts that column 26 lines 7 – 8 of the Deo reference disclose a broadcast key which is currently stored in a mobile device. Claim 11 of the current application discloses a first step of "initializing a control center and a receiver with a shared main key." Since this clause is the first step of a method claim, it establishes the initial state of the control center and the receiver, wherein both the control center and the receiver share a main key. Instead Deo discloses a process of programming mobile devices and changing broadcast keys in a multi step process to generate a message specific key (Fig. 8A, 8B, and 9A) and lacks disclosure of a control center and a receiver which share a main key in the initial state of the control center and the receiver.

The Examiner asserts that the Deo reference, Fig. 9A and column 26 lines 7 through 23 disclose a control center which produces a sequence number and wherein the sequence number and a main key produce a signing key. The Examiner also asserts that message specific data disclosed in Deo is equivalent to sequence numbers disclosed in the current application (second Office Action sec. 9). The Examiner has failed to recognize that Figure 9a and column 26 lines 7 -23 of the Deo reference refer to generation of encrypted content "once the mobile device has been programmed" with the new key (Deo column 25 lines 65 -67 and column 26 line 1). The Applicant points out that several intermediate steps are required in the Deo invention to produce a signing key such as the generation of hash values based on message specific data and an old key, biasing a key derivation algorithm, and providing a key

Appl. No. 09/720,353
Amendment dated April 8, 2005
Reply to Office Action of January 13, 2005

derivation algorithm to a key derivation component. Furthermore, Deo discloses hash values and key derivation algorithms rather than a sequence number.

The Examiner asserts that providing a signing key in advance is not found in Claim 11 (second Office Action sec. 10). The argument outlined above addressing sec. 6 of the second Office Action is also applicable to the Examiner's rejection in sec. 10.

Based on column 28 lines 1 - 4 of the Deo reference, the Examiner rejects Applicant's argument that the Deo reference does not disclose use of generated sequence numbers with the main key to generate a check key to verify the signature of the message in the receiver (second Office Action sec. 11). In the Deo reference, a "cryptographic service provider" decrypts a content message and provides it in an unencrypted form to a cryptography application programming interface (CAPI) which in turn provides a decrypted message back to a router (Deo reference column 28 lines 20 - 23). In addition, the decryption process disclosed in the Deo reference is such that encrypted content messages can be decrypted "for use by" a mobile device without a broadcast key ever leaving a driver. (Deo reference column 28 lines 46 - 48). Unlike Claim 11 of the current application, the Deo reference lacks disclosure of decryption of a message using a check key to verify a signature on the message, wherein the decryption is conducted in a receiver.

The Examiner asserts that the method step of Claim 11, as previously presented in Applicant's amendment dated June 30, 2004, "wherein the control center and the receiver share an undiscoverable main key," is taught by the Deo reference disclosure of a control center wherein the control center first obtains the current broadcast key which is currently stored on the receiver (second Office Action sec. 12). Since the control center "obtains" the broadcast key disclosed in Deo, the key is not undiscoverable. Furthermore, since the key is "obtained" from the mobile device it teaches the concept of transfer of a key, rather than sharing of a main key.

Appl. No. 09/720,353
Amendment dated April 8, 2005
Reply to Office Action of January 13, 2005

Consequently, the Applicant respectfully requests that the rejection of Claim 11 be withdrawn.

Dependent claims, by definition, further define the subject matter of the independent claims from which they depend. Because Claims 2 - 7 depend from Claim 11, Claims 2 - 7 further define the subject matter of independent Claim 11. Because Claim 11 is believed to be in a condition of allowance for at least the reasons presented above, Claims 2 - 7 are also believed to be allowable. Consequently, Applicant respectfully requests that the rejections of Claims 2 - 7 be withdrawn.

The Examiner rejects Claims 2 - 7, 9 and 11 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,608,800 to Hoffmann (second Office Action sec. 24 - 28).

The Hoffmann reference discloses a means for transmitting useful data from a transmitter to a receiver. The transmitter comprises useful data, a signature associated with the useful data, and a transfer key. The receiver contains a corresponding transfer key. The transfer key permits confidential transmission of random data. In order to safeguard the transmission of the useful data, the signature associated with the useful data is converted to an enciphered signature. A message transmitted from the transmitter to the receiver comprises coupling data, enciphered random data, the useful data and the enciphered signature.

The Hoffman reference further discloses generation of the message to be transmitted from the transmitter to the receiver in the following manner. First, random data are generated by a random data generator at the transmitter. Furthermore, coupling data are generated. A symmetric key is then generated from the random data and the coupling data by one-way enciphering. With the aid of the symmetric key, the signature associated with the useful data is symmetrically enciphered and the enciphered signature is generated. In addition, the random data are enciphered with the aid of the transfer key.

Appl. No. 09/720,353
Amendment dated April 8, 2005
Reply to Office Action of January 13, 2005

The Hoffmann reference further discloses checking of the transmitted message per the following steps. First, the coupling data is checked for plausibility and if discrepancies are revealed the message is rejected. Next, the random data are recovered by deciphering the enciphered random data with the aid of the transfer key. Using one-way enciphering, the symmetric key is determined from the calculated random data and the coupling data. By deciphering the enciphered signature with the aid of the symmetric key, the signature is recovered. The signature is then checked and if errors are revealed the message is rejected.

The Examiner rejects Claim 5, under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,608,800 to Hoffmann, asserting that column 3 lines 37 – 38 of the Hoffmann reference teach the limitations of Claim 5 (second Office Action sec. 26). The Applicant respectfully submits that the Hoffmann reference discloses “random data generated by a random data generator,” rather than a “sequence number produced by a pseudo-random number generator,” as disclosed in Claim 5 of the current application. A pseudo-random number generator is a type of deterministic algorithm utilized by random number generators.

Consequently, the Applicant respectfully requests that the rejection of Claim 5 be withdrawn.

The Hoffmann reference discloses a transmitter and a receiver rather than providing a control center, a sender and a receiver, as recited in Claim 11 of the current application. Unlike the invention recited in Claim 11 of the current application, Hoffman does not disclose an intermediate sender between the control center and receiver. Also unlike the invention recited in Claim 11 of the current application, Hoffmann does not disclose “causing the control center to produce one or more sequence number,” as disclosed in Claim 11. Instead, Hoffmann teaches the generation of random data at the transmitter. (See column 3 lines 37 - 38 of Hoffmann). The Examiner also fails to recognize that the Hoffmann reference discloses the use of both random data and coupling data to create a symmetric key

Appl. No. 09/720,353
Amendment dated April 8, 2005
Reply to Office Action of January 13, 2005

(Hoffmann reference column 3 lines 40 - 42), rather than "using one of the sequence numbers and the main key to create a signing key," as disclosed in Claim 11. The transfer key disclosed in the Hoffman reference is not involved in creating the signing key. Instead, Hoffmann discloses use of the transfer key to encipher and decipher random data (Hoffman reference column 3 lines 46 - 48 and lines 65 - 67).

Hoffman discloses a transfer key on the transmitter side and a "corresponding" transfer key on the receiver side (Hoffmann reference column 3 lines 20 - 23 and lines 53 - 57). The Hoffmann reference is absent disclosure of a control center and a receiver which share a main key as disclosed in Claim 11. The Applicant respectfully submits that the Hoffmann reference does not disclose "passing the sequence number through a one-time encryption to produce a check key and using the check key to verify the signature." Instead, the Hoffmann reference discloses the steps of checking coupling data; recovering random data by deciphering the encrypted random data with the aid of the transfer key; using a one-way enciphering to determine the symmetric key from the recovered random data; deciphering the enciphered signature with the aid of the symmetric key to recover the signature; and checking the signature (Hoffmann reference column 3 lines 60 - 67 and column 4 lines 1 - 7).

It is clear that the Hoffman reference requires both coupling data and random data to be checked rather than passing one sequence number through a one-time encryption process. The Hoffmann reference can be further distinguished from Claim 11 of the current application in that the Hoffmann reference discloses transmittal of a bulk message comprising useful data, an enciphered signature, coupling data and random data, but does not include the transmittal of any key (Hoffman reference column 3 lines 50 - 52). In contrast, Claim 11 discloses "providing the signing key and the sequence number to the sender via a secure transmission."

Appl. No. 09/720,353
Amendment dated April 8, 2005
Reply to Office Action of January 13, 2005

Consequently, the Applicant respectfully requests that the rejection of Claim 11 be withdrawn.

Because Claims 2 – 7 depend from Claim 11, the Applicant respectfully requests that the rejection of Claims 2 – 7 also be withdrawn.

The Examiner rejects Claim 9, under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,608,800 to Hoffmann (second Office Action sec. 28).

The Examiner asserts that the control center and receiver inherently use memory and that any data operation uses memory. Control centers and receivers do not necessarily have memories. For instance a control center could comprise a building or other structure, wherein there is no memory.

In addition, the Examiner asserts that the Hoffmann reference column 3, lines 35 – 36, reads on the Claim 9 clause “one input of a first one-time encrypter being connected to a generator for a sequence number.” However, the Hoffmann reference lacks disclosure of any connectivity between an encrypter and a generator.

The Applicant asserts that Claim 9 discloses additional degrees of connectivity between components not disclosed in the Hoffmann reference. The pertinent part of Claim 9 reads “one input of a first one-time encrypter being connected to the first memory of the control center, and another input being connected to a generator for a sequence number.” Connection of the components disclosed in claim 9 of the current invention is not inherent. The Hoffmann reference is silent on how the random data generated by the generator is introduced to the enciphering process. It is possible that the random data, referred to in the Hoffmann reference, is entered manually into the enciphering process and no connection exists.

The Examiner further asserts that the Hoffmann reference at column 3 lines 49 - 52 reads on the following pertinent part of Claim 9. “An output of the signature generator being connected to a device which assembles at least the signature and the message to form a data message block and whose output is connected to the receiver via a transport medium.” The Hoffmann reference lacks disclosure of “a device

Appl. No. 09/720,353
Amendment dated April 8, 2005
Reply to Office Action of January 13, 2005

which assembles at least the signature and the message." Accordingly, reconsideration is requested.

The Examiner also asserts that Figure 4 of the Hofmann reference discloses a "signature checker having inputs connected to the message and to the signature and an output of a second one-time encrypter and the input of the second one-time encrypter being connected to a means for providing a sequence number." Figure 4 depicts a solid line with an arrow pointing from only the useful data portion of the message to a signature checker, rather than "a signature checker provided in the receiver having inputs connected to the message," as disclosed in Claim 9 of the current application.

Consequently, the Applicant respectfully requests that the rejection of Claim 9 be withdrawn.

The Examiner rejects Claim 8 under U.S.C. 103(a) as being unpatentable over Hoffmann in view of Horstmann (second Office Action sec. 14).

The Horstmann reference discloses a mechanism for use in conjunction with Electronic Software Distribution (ESD) that provides purchase documentation and that allows for convenient re-download and re-licensing of software, including old software versions. In one embodiment of the invention, a re-licensing manager software utility installed on an end user's machine interacts with one or more of a remote publisher site, a licensing clearing house and a merchant site to re-license, transfer, or obtain a refund for a software product. The role of the license clearing house is to keep a count of licensed installations and to grant or deny permission to re-license based on the count. The clearing house keeps a list of sequence numbers to avoid replay attack.

In order to establish prima facie obviousness, one of the requirements is that the prior art references when combined must teach or suggest all of the claim limitations. The Horstmann reference does not teach a receiver which maintains a list of already used sequence numbers. Instead, the Horstmann reference teaches

Appl. No. 09/720,353
Amendment dated April 8, 2005
Reply to Office Action of January 13, 2005

away from a mobile device or receiver which maintains a list of already used sequence numbers by reciting that a central clearinghouse or product server maintain such a list.

Consequently, the Applicant respectfully requests that the rejection of Claim 8 be withdrawn.

The Examiner rejects Claim 10 under U.S.C. § 103(a) as being unpatentable over Hoffmann in view of Official Notice asserting that it is old and well known practice to use deterministic methods to produce numbers (second Office Action sec. 32 and 33). In order to establish prima facie obviousness, one of the requirements is that the prior art references when combined must teach or suggest all of the claim limitations. The Applicant believes that there exists a plurality of methods for generation of numbers and that there is no suggestion or motivation in the known practice of to use deterministic method for generation of sequence numbers that correspond to the same number of check keys.

Consequently, the Applicant respectfully requests that the rejection of Claim 10 be withdrawn.


Based on the foregoing and for at least these reasons, Applicants respectfully submit that claims of the application in question are in condition for allowance and an early action to that effect is earnestly solicited.

Should any matters remain unresolved, Applicants request that the Examiner contact Applicants' Representative at the number listed herein below.

Appl. No. 09/720,353
Amendment dated April 8, 2005
Reply to Office Action of January 13, 2005

While Applicants believe no fees are due upon filing this response, please charge any deficiencies in fees associated with this response to Deposit Account No. 503342.

Respectfully submitted,

By 
Richard R. Michaud
Registration No. 40,088
Attorney for Applicant

Michaud-Duffy Group LLP
CenterPoint
306 Industrial Park Road
Suite 206
Middletown, CT 06457-1532
(860) 632-7200